PAMを使用した認証

概要

この記事では、PAMのコンセプト、PAM設定の構造、およびPAMを設定するツールの使用法について説明します。

目的

PAMモジュールを設定し、U2Fキーを使用するようにシステムを設定する方法を理解する必要があります。

所要時間

この記事の理解には20分ほどを要します。

要件

- U2Fキーを使用して認証を設定するには、YubiKeyまたはセキュリティキーのいずれかが必要です。

発行日: 11/12/2025

目次

1 PAMの概要

通常、システム管理者とプログラマは、システムの一定部分へのアクセスを制限することや、アプリケーションの一定の機能の使用を制限することを望みます。PAMを使用しなければ、新規の認証メカニズム(LDAPやSamba、Kerberosなど)が導入されるたびにアプリケーションを調整する必要があります。ただし、このプロセスは時間がかかり、エラーが発生しやすくなります。このような難点を回避する方法の1つは、アプリケーションを認証メカニズムから分離し、認証は集中管理されるモジュールに任せることです。新しい認証方式が必要になった場合は、問題のプログラムで使用できるように適切なPAMモジュールを調整または記述するだけで済みます。

PAMのコンセプトは以下で構成されます。

- 「PAMモジュール」。特定の認証メカニズム用の共有ライブラリのセットです。
- 「モジュールスタック」。1つ以上のPAMモジュールで構成されます。
- PAM対応「サービス」。モジュールスタックまたはPAMモジュールを使用して認証する必要があります。通常、サービスは、**`login`**や**`su`**のように、対応するアプリケーションのよく知られた名前になっています。サービス名`other`は、デフォルトルール用の予約語です。
- 「モジュール引数」。これを使用して、1つのPAMモジュールの実行に影響を与えることができます。
- 1つのPAMモジュールの実行「結果」それぞれを評価するメカニズム。正の値は、次のPAMモジュールを実行します。負の値を処理する方法は、設定に応じて異なります。「no influence, proceed (影響なし、続行)」から「terminate immediately (直ちに終了)」までの任意のオプションが有効です。

2 PAM設定の構造

SLE MicroのPAMには、いわゆるディレクトリベースの設定が付属しています。設定ファイルのセットは`/etc/pam.d`に保存されます。PAMのメカニズムに依存するすべてのサービス(またはプログラム)には、専用の設定ファイルがこのディレクトリにあります。たとえば、`sshd`用のサービスは`/etc/pam.d/sshd`ファイルにあります。

注記: SLE Microではファイルベースの設定(/etc/pam.conf)は使用されない

各サービスの設定を/etc/pam.confに保存することもできます。ただし、保守と使いやすさの理由から、この設定スキームはSLE Microでは使用されません。

/etc/pam.d/の下層にあるファイルでは、認証に使用するPAMモジュールが定義されます。各ファイルはサービスを定義する行で構成され、各行は最大で4つの要素で構成されます。

```
TYPE
CONTROL
MODULE_PATH
MODULE_ARGS
```

各要素には次のような意味があります。

TYPE

サービスのタイプを宣言します。PAMモジュールはスタックとして処理されます。モジュールのタイプによって目的が異なります。たとえば、あるモジュールはパスワードをチェックし、他のモジュールはシステムがアクセスされた場所を検証し、また別のモジュールはユーザ固有の設定を読み込みます。PAMは、次の4タイプのモジュールを認識します。

auth

パスワードを問い合わせる従来の方法で、ユーザの真正性を確認します。ただし、これはチップカードや生体認証(たとえば指紋や虹彩スキャン)によっても実行できます。

account

このタイプのモジュールは、ユーザがリクエストしたサービスを使用するための一般許可を付与されているかどうかをチェックします。たとえば、失効したアカウントのユーザ名では誰もログインできないようにするには、この種のチェックを実行する必要があります。

password

このタイプのモジュールの目的は、認証トークンを変更可能にすることです。通常、これはパスワードです。

session

このタイプのモジュールは、ユーザセッションの管理と設定を受け持ちます。認証の前後に起動し、ログイン試行をログに記録して、ユーザ固有の環境を設定します。

CONTROL

PAMモジュールの動作を指定します。各モジュールには次の制御フラグを設定できます。

required

このフラグが付いているモジュールは、認証を進める前に正常に処理される必要があります。requiredフラグが付いたモジュールが失敗すると、同じフラグが付いた他のモジュールがすべて処理されてから、認証の失敗に関するメッセージがユーザに返されます。

requisite

このフラグが付いているモジュールも、requiredフラグが付いている場合とほぼ同様に、正常に処理される必要があります。ただし、このフラグが付いたモジュールが失敗した場合は、ユーザに即座にフィードバックが送られ、他のモジュールは処理されません。成功すると、requiredフラグが付いているモジュールの場合と同様に、続いて他のモジュールが処理されます。requisiteフラグは、正しい認証に不可欠な一定条件の有無を確認するための基本フィルタとして使用できます。

sufficient

このフラグが付いたモジュールが正常に処理されると、呼び出し元アプリケーションは即時に成功メッセージを受け取り、前にrequiredフラグが付いたモジュールが失敗していなければ、他のモジュールは処理されません。sufficientフラグが付いたモジュールが失敗しても、直接的な結果は発生せず、以降のモジュールはそれぞれの順序で処理されます。

optional

このフラグが付いたモジュールが成功しても失敗しても、直接的な影響はありません。このフラグは、それ以上はアクションを実行しない、メッセージ表示(ユーザへのメール着信通知など)専用のモジュールに便利です。

include

このフラグが設定された場合、引数として指定されたファイルがこの場所に挿入されます。

MODULE_PATH

PAMモジュールの完全なファイル名が含まれます。モジュールがデフォルトのディレクトリ/lib/securityにある場合は、明示的に指定する必要はありません(SLE Microがサポートするすべての64ビットプラットフォームでは、このディレクトリは/lib64/securityです)。

MODULE_ARGS

: debug (デバッグの有効化)やnullok (空のパスワードの使用を許可)など、PAMモジュールの動作に影響を与えるオプションのスペース区切りリストが含まれます。

さらに、/etc/securityの下にPAMモジュールのグローバル設定ファイルがあり、これらのモジュールの正確な動作を定義しています(たとえば、pam_env.confやtime.confです)。PAMモジュールを使用する各アプリケーションは、一連のPAM関数を呼び出し、各PAM関数は設定ファイルの情報を処理して、その結果を呼び出し元のアプリケーションに戻します。

PAMモジュールの作成と保守を簡素化するために、auth、account、password、およびsessionのタイプのモジュールに共通のデフォルト設定ファイルが導入されました。これらのファイルは、すべてのアプリケーションのPAM設定から取得されます。common-*でグローバルPAM設定モジュールを更新すると、すべてのPAM設定ファイルに更新が伝播されるため、管理者はすべてのPAM設定ファイルをひとつひとつ更新せずに済みます。

グローバルPAM設定ファイルは、**pam-config**ツールを使用して管理されます。このツールは、新しいモジュールを設定に自動的に追加したり、既存のモジュールの設定を変更したり、設定からモジュール(またはオプション)を削除したりします。PAM設定を管理する際に手動で介入する必要は、最小限しかないか、まったくありません。

2.1 PAM設定の例

PAM設定の実際のユースケースを示すために、このセクションではsshdの設定を使用します。

例 1: SSHDのPAM設定(/etc/pam.d/sshd)

```
#%PAM-1.0 ❶
auth     requisite      pam_nologin.so                          ❷
auth     include        common-auth                             ❸
account  requisite      pam_nologin.so                          ❷
account  include        common-account                          ❸
password include        common-password                         ❸
session  required       pam_loginuid.so                         ❹
session  include        common-session                          ❸
session  optional       pam_lastlog.so   silent noupdate showfailed ❺
```

❶ PAM 1.0用のこの設定ファイルのバージョンを宣言します。これは単に慣習ですが、今後バージョンを確認するために使用できます。

❷ /etc/nologinが存在するかどうかを確認します。存在しない場合、root以外のユーザはログインできません。

❸ common-auth、common-account、common-password、common-sessionの4つのモジュールタイプの設定ファイルを参照します。これら4つのファイルにはそれぞれのモジュールタイプ用のデフォルト設定があります。

❹ 認証されたプロセスのログインUIDプロセス属性を設定します。

❺ ユーザの最終ログインに関する情報を表示します。

各モジュールをそれぞれのPAM設定に個別に追加するのではなく設定ファイルを含めることにより、管理者がデフォルト値を変更した場合に、更新されたPAM設定が自動的に取得されます。

最初のインクルードファイル(common-auth)は、authタイプのモジュールであるpam_env.so、pam_gnome_keyring.so、およびpam_unix.soを呼び出します。例2「authセクションのデフォルト設定(common-auth)」を参照してください。モジュールはインストールによって異なる場合があることに注意してください。

例 2: authセクションのデフォルト設定(common-auth)

```
auth  required  pam_env.so                  ❶
auth  optional  pam_gnome_keyring.so        ❷
auth  required  pam_unix.so  try_first_pass ❸
```

❶ pam_env.soは、/etc/security/pam_env.confをロードして、このファイルで指定されているとおりに環境変数を設定します。pam_envモジュールはログイン元を認識するため、このファイルを使用するとDISPLAY変数を適切な値に設定できます。

❷ pam_gnome_keyring.soは、ユーザのログインとパスワードをGNOMEキーリングと照合します。

❸ pam_unixは、ユーザのログイン名とパスワードを/etc/passwdおよび/etc/shadowと照合します。

sshdがログインの成否に関するフィードバックを受け取る前に、authモジュールのスタック全体が処理されます。sshdが成功のメッセージを受け取る前に、制御フラグrequiredが設定されたスタックのすべてのモジュールが正常に処理される必要があります。モジュールの1つが失敗した場合もモジュールスタック全体が同様に処理され、その後にのみsshdに失敗が通知されます。

authタイプのすべてのモジュールが正常に処理された時点で、別のinclude文が処理されます。この例では例3「accountセクションのデフォルト設定(common-account)」になります。common-accountには、1つのモジュール、pam_unixのみが含まれます。pam_unixからユーザが存在するという結果が戻されると、sshdは成功したことを通知するメッセージを受信し、モジュールの次のスタック(password)が処理されます。

例 3: accountセクションのデフォルト設定(common-account)

```
account  required  pam_unix.so  try_first_pass
```

繰り返しになりますが、sshdのPAM設定はcommon-passwordにあるpasswordモジュールのデフォルト設定を参照する1つのinclude文にのみ関係します。アプリケーションが認証トークンの変更をリクエストするたびに、これらのモジュールを正常に完了する必要があります(制御フラグrequisiteおよびrequired)。

パスワード変更や別の認証トークンについてはセキュリティチェックが必要です。これは、pam_cracklibモジュールで実行されます。その後に使用されるpam_unixモジュールは、pam_cracklibから新旧のパスワードを引き継ぐため、ユーザはパスワードの変更後に再度認証する必要はありません。この手順により、pam_cracklibによるチェックを回避することはできなくなります。accountまたはauthのタイプが失効したパスワードについて通知するように設定されている場合は、passwordモジュールも使用する必要があります。

最終ステップとして、(common-sessionファイルに組み込まれた) sessionタイプのモジュールが呼び出され、問題のユーザ用の設定に従ってセッションが設定されます。pam_limitsモジュールは、特定のシステムリソースの使用に対する制限を定義するファイル/etc/security/limits.confをロードします。pam_unixモジュールが再度処理されます。pam_umaskモジュールを使用して、ファイルモード作成マスクを設定できます。このモジュールにはoptionalフラグが付いているため、このモジュールが失敗しても、セッションモジュールスタック全体の正常な完了には影響しません。sessionモジュールはユーザのログアウト時に再び呼び出されます。

3 PAMモジュールの設定

設定可能なPAMモジュールもあります。設定ファイルは/etc/securityにあります。このセクションでは、sshdの例に関連する設定ファイルpam_env.confとlimits.confについて簡単に説明します。

3.1 pam_env.conf

pam_env.confを使用すると、pam_envモジュールが呼び出されるたびに設定される、ユーザ用に標準化された環境を定義できます。それにより、次の構文を使用して環境変数を事前設定できます。

```
VARIABLE  [DEFAULT=VALUE]  [OVERRIDE=VALUE]
```

`VARIABLE`
: 設定する環境変数の名前です。

`[DEFAULT=<value>]`
: 管理者が設定するデフォルト`VALUE`。

`[OVERRIDE=<value>]`
: 問い合わせ可能で`pam_env`によって設定される値です。この値でデフォルト値が上書きされます。

`pam_env`の典型的な使用例は、`DISPLAY`変数の取得です。これは、リモートログインが行われるたびに変更されます。これを例4「pam_env.conf」に示します。

例 4: PAM_ENV.CONF

```
REMOTEHOST  DEFAULT=localhost          OVERRIDE=@{PAM_RHOST}
DISPLAY     DEFAULT=${REMOTEHOST}:0.0  OVERRIDE=${DISPLAY}
```

1行目では、`REMOTEHOST`変数の値が`localhost`に設定されており、`pam_env`が他の値を判別できない場合にこの値が使用されます。`DISPLAY`変数には、`REMOTEHOST`の値が含まれています。詳細については、`/etc/security/pam_env.conf`のコメントを参照してください。

3.2 limits.conf

`limits.conf`では、ユーザ別またはグループ別のシステム制限を設定できます。このファイルは、`pam_limits`モジュールに読み込まれます。このファイルを使用すると、超過できない厳密な制限と、一時的な超過が許される緩やかな制限を設定できます。構文およびオプションの詳細については、`/etc/security/limits.conf`のコメントを参照してください。

4 pam-configを使用したPAMの設定

`pam-config`ツールは、グローバルなPAM設定ファイル(`/etc/pam.d/common-*`)と、選択されたいくつかのアプリケーション設定を構成するのに役立ちます。サポートされているモジュールのリストについては、**`pam-config --list-modules`**コマンドを使用してください。**`pam-config`**コマンドを使用して、PAM設定ファイルを管理します。新しいモジュールをPAM設定に追加したり、他のモジュールを削除したり、これらのモジュールのオプションを変更したりします。グローバルなPAM設定ファイルを変更する場合、個々のアプリケーションのPAMセットアップを手動で調整する必要はありません。

`pam-config`のシンプルなユースケースには次のようなものがあります。

1. **Unixスタイルの新しいPAM設定を自動生成します。** `pam-config`で可能な限り単純なセットアップを作成し、後で拡張できるようにします。`pam-config --create`コマンドは、単純なUnix認証設定を作成します。`pam-config`で管理されていない既存の設定ファイルは上書きされますが、バックアップコピーは`*.pam-config-backup`として保持されます。
2. **新しい認証方法を追加します。** 新しい認証方法(たとえば、LDAP)をPAMモジュールのスタックに追加するには、単純な`pam-config --add --ldap`コマンドを実行します。LDAPは、すべての`common-*-pc` PAM設定ファイルの該当する箇所に追加されます。
3. **テストのためにデバッグを追加します。** 新しい認証手順が計画どおりに動作することを確認するために、すべてのPAM関連操作のデバッグをオンにします。`pam-config --add --ldap-debug`で、LDAP関連のPAM操作のデバッグをオンにします。
4. **セットアップを問い合わせます。** 最終的に新しいPAMセットアップを適用する前に、追加したいすべてのオプションが含まれているかどうかを確認します。`pam-config --query --MODULE`コマンドで、問い合わせたPAMモジュールのタイプとオプションの両方を一覧にします。
5. **デバッグオプションを削除します。** 最後に、セットアップのパフォーマンスにまったく問題がない場合は、デバッグオプションをセットアップから削除します。`pam-config --delete --ldap-debug`コマンドで、LDAP認証のデバッグをオフにします。他のモジュールにデバッグオプションを追加していた場合は、同様のコマンドを使用してオフにします。

`pam-config`コマンドと利用可能なオプションの詳細については、`pam-config(8)`のマニュアルページを参照してください。

5 PAMの手動設定

PAM設定ファイルを手動で作成または管理したい場合は、これらのファイルの`pam-config`を無効にしてください。

`pam-config --create`コマンドを使用して最初からPAM設定ファイルを作成すると、`common-*`から`common-*-pc`ファイルへのシンボリックリンクが作成されます。`pam-config`は、`common-*-pc`の設定ファイルのみを変更します。これらのシンボリックリンクを削除すると、`pam-config`は事実上無効になります。これは、`pam-config`は`common-*-pc`ファイルのみを処理し、これらのファイルはシンボリックリンクなしでは有効にならないためです。

警告: pam_systemd.soを設定に含める

独自のPAM設定を作成する場合は、`session optional`として設定したpam_systemd.soを含めるようにしてください。pam_systemd.soを含めないと、systemdのタスク制限に問題が発生する可能性があります。詳細については、pam_systemd.soのマニュアルページを参照してください。

6 ローカルログイン用のU2Fキーを要求するためのSLE Microの設定

SLE Microへのローカルログイン時のセキュリティを強化するために、pam-u2fフレームワーク、およびYubiKeyとセキュリティキーのU2F機能を使用して2要素認証を設定できます。

SLE MicroシステムでU2Fを設定するには、キーをSLE Microのアカウントに関連付ける必要があります。その後、このキーを使用するようにシステムを設定します。この手順については、次のセクションで説明します。

6.1 アカウントへのU2Fキーの関連付け

U2Fキーをアカウントに関連付けるには、次の手順に従います。

1. マシンにログインします。
2. U2Fキーを挿入します。
3. U2Fキーの設定用のディレクトリを作成します。

```
> sudo mkdir -p ~/.config/Yubico
```

4. 設定行を出力する**pamu2fcfg**コマンドを実行します。

```
> sudo pamu2fcfg > ~/.config/Yubico/u2f_keys
```

5. デバイスが点滅し始めたら、金属製の接点に触れて関連付けを確認します。

バックアップ用のU2Fデバイスを使用することをお勧めします。これは、次のコマンドを実行して設定できます。

1. 次のスクリプトを実行します。

```
> sudo pamu2fcfg -n >> ~/.config/Yubico/u2f_keys
```

2. デバイスが点滅し始めたら、金属製の接点に触れて関連付けを確認します。

セキュリティを強化するために、出力ファイルをデフォルトの場所から、ファイルを変更するためにsudo許可が必要なディレクトリに移動できます。たとえば、/etcディレクトリに移動します。これを行うには、次の手順に従います。

1. /etcにディレクトリを作成します。

```
> sudo mkdir /etc/Yubico
```

2. 作成したファイルを移動します。

```
> sudo mv ~/.config/Yubico/u2f_keys /etc/Yubico/u2f_keys
```

注記: u2f_keysをデフォルト以外の場所に配置する

出力ファイルをデフォルト($HOME/.config/Yubico/u2f_keys)とは異なるディレクトリに移動する場合は、6.2項 「PAM設定の更新」の説明に従って、/etc/pam.d/loginファイルにパスを追加する必要があります。

6.2 PAM設定の更新

U2Fキー設定を作成した後で、システムのPAM設定を調整する必要があります。

1. ファイル/etc/pam.d/loginを開きます。
2. このファイルに、次のようにauth required pam_u2f.soという行を追加します。

```
#%PAM-1.0
auth       include    common-auth
auth       required   pam_u2f.so
account    include    common-account
password   include    common-password
session    optional   pam_keyinit.so revoke
session    include    common-session
#session   optional   pam_xauth.so
```

3. u2f_keysファイルを$HOME/.config/Yubico/u2f_keysとは異なる場所に配置した場合は、次のように、/etc/pam.d/loginのPAMファイルでauthfileオプションを使用する必要があります。

```
#%PAM-1.0
auth     requisite pam_nologin.so
auth     include   common-auth
auth  required pam_u2f.so authfile=<PATH_TO_u2f_keys>
...
```

ここで、<PATH_TO_u2f_keys>はu2f_keysファイルの絶対パスです。

7 法的事項

A GNUフリー文書利用許諾契約書(GFDL)

0. 序文

この利用許諾契約書の目的は、マニュアル、テキストブック、またはその他の機能的で有用な文書を、自由という意味で「フリー」にすることです。つまり、そのような文書を、変更の有無や商用非商用に関わらず、コピーまたは再配布する実効的な自由をすべての人々に保証することです。第二に、本利用許諾契約書は、作者または発行者が他者によって行われた変更について責任を負わないとともに、その著作物の功績が確保されるように意図されています。

本利用許諾契約書は、「コピーレフト」(著作物を自由に複製および改変できるようにすること)の一種であり、文書の派生著作物は、それ自体が同じ意味においてフリーでなければなりません。フリーソフトウェア向けに考慮されたコピーレフト利用許諾であるGNU一般公衆利用許諾契約書(GPL)を補足するものです。

弊社は、この利用許諾契約書をフリーソフトウェアのマニュアルに使用するために設計しました。それは、フリーソフトウェアにはフリーマニュアルが必要であるためです。つまり、フリープログラムには、そのソフトウェアと同じ自由を提供するマニュアルが付属しなければなりません。ただし、本利用許諾契約書は、ソフトウェアマニュアルに制限されるものではありません。主題であるか否か、または印刷された本として発行されるか否かに関わらず、任意のテキスト著作物に使用することができます。本利用許諾契約書は、その目的が指示または参照に置かれている著作物に主に使用することを推奨します。

1. 適用範囲と定義

本利用許諾契約書は、この利用許諾の条項に従って頒布できることを定めた著作権者の通告が記載されている任意のメディアにおけるマニュアルまたは他の著作物に適用されます。そのような通告は、その著作物をここに記載されている条件に従って使用するための世界的な無償の利用許諾を無期限で付与します。次に示す「文書」は、そのような任意のマニュアルまたは著作物を指します。その公衆ユーザはいずれも被許諾者であり、「利用者」と呼ばれます。利用者は、著作権法に従った許可が必要になるような方法で著作物を複製、変更または頒布する場合に、利用許諾を受け入れます。

文書の「変更された版」とは、そのまま複製されるか、変更または別の言語に翻訳された(またはその両方)文書あるいはその一部を含んだ著作物のことです。

「二次セクション」は、文書の発行者または作者と文書の全体的な主題(または関連事項)との関係のみを示す文書の名前付き付録または前付け部分です。総体的な主題に直接関わる内容は含まれていません。(したがって、文書が部分的に数学のテキストブックになっている場合、二次セクションでは数学について説明されない場合があります)。関係には、主題または関連事項との歴史的なつながり、あるいはそれらに関する法的、商的、哲学的、倫理的、政治的位置付けが含まれる場合があります。

「不変セクション」は、文書が本利用許諾契約書の条件の下でリリースされる旨を述べている通告において、そのタイトルが不変セクションのものとして指定されている、ある特定の二次セクションです。セクションが、すでに説明した二次セクションの定義に一致しない場合は、不変として指定することはできません。文書には、不変セクションが含まれない場合があります。文書で不変セクションを特定しない場合、不変セクションは含まれません。

「カバーテキスト」とは、文書が本利用許諾契約書の条件の下でリリースされる旨を述べている通告において、表カバーテキストまたは裏カバーテキストとして列挙されている、ある一定の短い文章のことです。表カバーテキストは、最大で5語、裏カバーテキストは、最大で25語によって構成できます。

文書の「透過的な複製」とは、その仕様が一般の利用者にとって入手可能で、一般的なテキストエディタまたは一般的な描画プログラム(画素で構成される画像用)、あるいは広く使用されている図面エディタ(図面用)で文書を直接改訂するのに適した形式で表される機械可読の複製のことです。テキストフォーマッタへの入力またはテキストフォーマッタへの入力に適したさまざまな形式への変換に適していることも前提になります。読者による以後の変更を阻止または妨げるようにマークアップまたはマークアップのない状態が調整されている、他の点では透過的なファイル形式で行われた複製は、透過的な複製ではありません。イメージ形式は、相当量のテキストに使用されている場合、透過的ではありません。「透過的」ではない複製は、「不透明」と呼ばれます。

透過的な複製に適した形式として、マークアップのないプレーンなASCII、Texinfo入力形式、LaTeX入力形式、一般に取得可能なDTDを使用するSGMLまたはXML、標準に準拠したHTML、人為的変更用のPostScriptまたはPDFがあります。透過的なイメージ形式には、PNG、XCF、JPGが含まれます。不透明な形式には、独自のワードプロセッサのみで読み取りおよび編集を行える独自の形式、DTDまたは処理(またはその両方)ツールを一般に取得できないSGMLまたはXML、機械生成HTML、出力のみを目的として一部のワードプロセッサによって作成されるPostScriptまたはPDFが含まれます。

「タイトルページ」とは、印刷された本の場合、タイトルページ自体、および本利用許諾契約書でタイトルページに表示することが要求されるマテリアルを読みやすいように保持するために必要な以降のページのことを指します。そのようなタイトルページがない形式の著作物の場合、「タイトルページ」は、本文の開始部分に先行する、著作物のタイトルを最も顕著に表している部分の近くにあるテキストのことを指します。

「XYZという表題の付いた」セクションとは、そのタイトルが正確にXYZになっているか、またはXYZを別の言語に翻訳しているテキストに続いてカッコ付きのXYZが含まれている文書の名前付きサブユニットのことです。(ここで、XYZは、次に示すように、「謝辞」、「献辞」、「推薦」、「履歴」などの特定のセクション名を表します)。文書を変更するときに、そのようなセクションの「タイトルを保存する」とは、この定義に従って「XYZという表題の付いた」セクションが残されることを表します。

文書では、本利用許諾契約書が文書に適用される旨を述べている通告の付近に保証の放棄を含めることができます。保証の放棄条項は、本利用許諾契約書内の参照によって、保証の放棄に関してのみ組み込まれると見なされます。つまり、これらの保証の放棄条項がもつ可能性のある他のいかなる含意も無効であり、本利用許諾契約書の意味にまったく影響を与えません。

2. そのままの複製

利用者は、商用か否かを問わず、任意のメディアにおいて文書を複製または頒布することができます。その際に、本利用許諾契約書、著作権表示、および本利用許諾契約書が文書に適用される旨を述べる利用許諾通告をすべての複製で再生し、本利用許諾契約書の条件に他のいかなる条件も追加しないことが前提条件になります。利用者は、技術的手段によって、作成または頒布する複製の読み込みまたはさらなる複製を妨げたり、制御したりすることはできません。ただし、複製と引き換えに対価を受け取ることができます。十分に大量の複製を頒布する場合は、セクション3の条件に従う必要もあります。

すでに述べた同じ条件に従って複製を貸与したり、複製を公開したりすることもできます。

3. 大量の複製

発行する文書の印刷した複製(または、通常、印刷したカバーをもつメディアに含まれた複製)が 100部を超え、文書の利用許諾通告でカバーテキストを必要とする場合は、すべてのカバーテキスト(表カバーの表カバーテキスト、裏カバーの裏カバーテキスト)を明瞭かつ読みやすく記載したカバーに文書の複製を同封する必要があります。また、両方のカバーでは、これらの複製の発行者として、利用者を読みやすい状態で明確に識別しなければなりません。表カバーには、フルタイトルを記述し、タイトルのすべての語が同等に目立つようにする必要があります。カバーには他のマテリアルを追加することもできます。カバーに限って変更を行った場合の複製は、文書のタイトルが保持されていて、これらの条件を満たしている限り、他の点に関してそのままの複製と見なすことができます。

いずれかのカバーで、必要なテキストが多すぎて、読みやすい状態に収まらない場合は、列挙されている最初の部分(問題なく収まる分)を実際のカバーに記載し、残りの部分を隣接ページに入れます。

文書の不透明な複製を100部以上公開または頒布する場合は、それぞれの不透明な複製とともに機械可読の透過的な複製を含めるか、それぞれの不透明な複製内あるいはその複製とともに、ネットワークの一般利用者が標準的な一般ネットワークプロトコルを使用して、追加マテリアルのない文書の完全な透過的複製をダウンロードするときにアクセスできるコンピュータネットワークの場所を明記する必要があります。後者のオプションを使用する場合は、不透明な複製の大量頒布を開始するときに十分慎重な手順を取り、この透過的な複製が、その版の不透明な複製を最後に一般頒布した後(直接またはエージェントや小売業者を通じて)少なくとも1年間、指定した場所で継続的にアクセス可能となるように配慮する必要があります。

大量の複製を再頒布する時点よりもかなり前に、文書の作者に連絡して、文書の更新版を提供する機会を与えることが要求されますが、必須ではありません。

4. 変更

文書の変更された版を、すでに述べた第2項および第3項の条件に従って複製および頒布することができます。その際は、本利用許諾契約書に確実に従って、変更された版をリリースし、変更された版が文書の役割を担うようにして、その複製を所要する任意の利用者に変更された版の頒布および変更の利用許諾を与えることが前提になります。また、変更された版で次のことを行う必要があります。

A. タイトルページ(カバーがある場合はカバー上も含める)で、文書、および以前の版の文書(以前の版がある場合は、その旨、文書の履歴セクションに列挙する)と識別されるタイトルを使用します。前の版と同じタイトルは、その版の元の発行者が許可を与えた場合に、使用することができます。

B. タイトルページ上に、この要件から解放されない限り、変更された版において変更の著者としての責任を担う1人以上の人またはエンティティとともに、文書の筆頭著者を少なくとも5人、作者として列挙します(5人に満たない場合は、その筆頭著者のすべて)。

C. タイトルページ上に、変更された版の発行者の名前を、発行者として記載します。

D. 文書のすべての著作権表示を保持します。

E. 変更に関する適切な著作権表示を、他の著作権表示の隣に追加します。

F. 著作権表示の直後に、本利用許諾契約書の条項に従って変更された版を利用するための許可を一般利用者に与える利用許諾通告を、次の補遺に示す形式で含めます。

G. その利用許諾通告に、不変セクションの全リスト、および文書の利用許諾通告で指定されている必須カバーテキストを保持します。

H. 本利用許諾契約書の変更されていない複製を含めます。

I. 「履歴」という表題のセクションを保持して、そのタイトルを保持し、タイトルページに記載されているとおりに、変更された版のタイトル、年度、新しい作者、発行者を少なくとも示す項目を追加します。文書に履歴というセクションがない場合は、そのタイトルページに記載されているとおりに文書のタイトル、年度、作者、発行者を示すセクションを作成し、前の文章に記載されているとおりに変更された版を示す項目を追加します。

J. 文書の透過的な複製に一般利用者がアクセスできるように文書で指定されている場合は、そのネットワークの場所、およびその文書の基盤となった前の版に対応して文書で指定されているネットワークの場所を保持します。これらは、「履歴」セクションに配置することができます。文書自体よりも4年以上前に発行された著作物の場合、または参照されているその版の元の発行者が許可を与えている場合は、そのネットワークの場所を省略することができます。

K. 「謝辞」または「献辞」という表題のセクションの場合は、そのセクションのタイトルを保持し、セクション内に、それぞれの貢献者謝辞またはその中の献辞(またはその両方)のすべての内容と意味合いを保持します。

L. 文書のすべての不変セクションを保持し、そのテキストおよびタイトルを未変更のままにします。セクション番号またはそれと同等の要素は、セクションタイトルの一部と見なされません。

M. 「推薦」という表題の任意のセクションを削除します。そのようなセクションは、変更された版に含めることはできません。

N. 既存のセクションのタイトルを変更して、「推薦」という表題にしたり、タイトルが不変セクションと矛盾したりしないようにします。

O. 保証の放棄を保持します。

変更された版に、二次セクションと見なされ、文書から複製されたマテリアルを含まない新しい前付けセクションまたは付録が含まれる場合は、これらの一部またはすべてを任意に「不変」として指定することができます。これを行うには、変更された版の利用許諾表示内で列挙されている不変セクションにそのタイトルを追加します。これらのタイトルは、他のすべてのセクションタイトルと異なっている必要があります。

「推薦」という表題のセクションを追加することができますが、その際は、変更された版のさまざまな当事者による推薦以外の要素が含まれていないことが前提になります。たとえば、校正者によるコメント、または文が標準的な信頼できる定義として組織によって承認されていることを示すという宣言文などが相当します。

表カバーテキストとしての最大5語の短い文、および裏カバーテキストとしての最大25語の短い文を、変更された版のカバーテキストのリストの終わりに追加できます。表カバーテキストの短い1文および裏カバーテキストの短い1文のみを、1つのエンティティが追加できます(またはエンティティによって行われた調整を通じて)。文書に、利用者または利用者が関わる同じエンティティによって行われた調整を通じて前に追加された同じカバーのカバーテキストがすでに含まれている場合は、別のものを追加することはできませんが、古いものを置き換えることができます。ただし、その古いものを追加した前の発行者から明示的な許可を得る必要があります。

文書の作者および発行者は、本利用許諾契約書により、その名前を得るために使用したり、変更された版の推薦を主張または暗示したりする許可を与えるものではありません。

5. 文書の結合

文書は、すでに述べた変更された版に関するセクション4の条件に従って、本利用許諾契約書の下でリリースされた他の文書と結合することができます。その際は、その組み合わせの中に、元の全文書のすべての不変セクションを未変更のまま含めて、そのすべてを結合された著作物の不変セクションとしてその利用許諾表示に列挙し、そのすべての保証の放棄を保持することが前提となります。

結合された著作物には、本利用許諾契約書の複製を1つのみ含める必要があります。複数の同一の不変セクションは、単一の複製で置き換えることができます。同じ名前だが内容の異なる複数の不変セクションがある場合は、そのような各セクションのタイトルを固有なものにします。その際は、その終わりに、カッコ付きで、そのセクションの元の作者または発行者の名前(既知の場合)、あるいは固有の番号を追加します。不変セクションのリスト内のセクションタイトルには、結合された著作物の利用許諾表示の場合と同じ調整を加えます。

組み合わせでは、さまざまな元の文書の「履歴」という表題のセクションを結合して、1つの「履歴」というセクションを構築する必要があります。同じように、「謝辞」という表題のセクション、および「献辞」という表題のセクションも結合します。「推薦」という表題のすべてのセクションを削除する必要があります。

6. 文書のコレクション

文書および本利用許諾契約書の下でリリースされた他の文書から成るコレクションを作成して、さまざまな文書に含まれる本利用許諾契約書の個々の複製を、コレクションに含まれる単一の複製で置き換えることができますが、他のすべての点での各文書のそのままの複製に関する本利用許諾契約書の規則に従うことが前提になります。

そのようなコレクションから単一の文書を抽出して、その文書を本利用許諾契約書に従って個々に頒布することができますが、その際は、本利用許諾契約書の複製を抽出した文書に挿入して、その文書のそのままの複製に関するその他のすべての点で、本利用許諾契約書に従う必要があります。

7. 独立した著作物の集積

文書またはその派生物を他の個別および独立した文書または著作物とともに、ストレージまたは頒布メディア内またはそのボリューム上に蓄積することを「集積」と呼びます。その場合は、個々の著作物の許可を超えてその蓄積の利用者の法的権限を制限することに、蓄積による著作権を使用しないことが前提になります。文書が集積に含まれる場合、本利用許諾契約書は、それ自体が文書の派生著作物ではない集積内の他の著作物に適用されません。

セクション3のカバーテキスト要件が文書のこれらの複製に適用可能であり、文書が集積全体の半分に満たない場合は、文書のカバーテキストを、集積内の文書のカバー、または文書が電子形式の場合は、電子的な同等のカバーに配置することができます。それ以外の場合は、集積全体の印刷されたカバー上に表示する必要があります。

8. 翻訳

翻訳は一種の変更と見なされるため、セクション4の条件に従って文書の翻訳を配布することができます。不変セクションを翻訳で置き換えるには、著作権者からの特別な許可が必要ですが、これらの不変セクションの元のバージョンのほかに、一部またはすべての不変セクションの翻訳を含めることができます。本利用許諾契約書、文書内のすべての利用許諾表示、および保証の放棄の翻訳を含めることができますが、その際は、本利用許諾契約書の元の英語版、およびそれらの利用許諾表示と保証の放棄の元の版も含めることが前提になります。本利用許諾契約書、利用許諾表示、または保証の放棄の翻訳と元の版との間に不一致がある場合は、元の版が優先されます。

文書内のセクションに、「謝辞」、「献辞」、または「履歴」という表題が付いている場合は、そのタイトルを保持する(セクション1)ための要件(セクション4)により、通常は実際のタイトルを変更する必要があります。

9. 終了

利用者は、本利用許諾契約書に明示的に記載されている形態を除き、文書を複製、改変、二次利用許諾、および頒布してはなりません。別の方法で文書を複製、改変、二次利用許諾、または頒布しようとするのは無効であり、本利用許諾契約書の下で利用者の権利は自動的に消滅します。ただし、本使用許諾の下で利用者から複製物または権利を受領した関係者は、条項を遵守している限り、権利が消滅することはありません。

10. 本利用許諾契約書の将来の改訂

フリーソフトウェア財団は、GNUフリー文書利用許諾契約書(GFDL)の新版または改訂版を随時公表することがあります。そのような新版は、性格的には現行版と似たものになりますが、新たな問題や懸案事項に対応するために細部が異なる可能性があります。https://www.gnu.org/copyleft/を参照してください。

本利用許諾契約書の各版には、区別するための版番号が設定されます。文書に、それに適用される本利用許諾契約書の特定の版番号と「後継版」が指定されている場合、利用者は、選択によって、その指定された版の条項またはフリーソフトウェア財団から公開される後継版の条

項(ドラフトではない)に従うことになります。文書に、本利用許諾契約書の版番号が指定されていない場合、利用者は、フリーソフトウェア財団からこれまでに公開された任意の版(ドラフトではない)を選択することができます。

補遺: 本利用許諾書をご使用の文書に使用する方法

```
Copyright (c) YEAR YOUR NAME.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.2
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled “GNU
Free Documentation License”.
```

不変セクション、表カバーテキスト、および裏カバーテキストがある場合は、「with...Texts」の行を次のように置き換えます。

```
with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.
```

カバーテキストのない不変セクションが含まれている場合、またはこの3つの他の組み合わせの場合は、その2つの代替要素をマージして状況に合わせます。

文書にプログラムコードの重要な例が含まれている場合は、GNU一般公衆利用許諾契約書(GPL)などの選択したフリーソフトウェアの利用許諾に従って、これらの例を平行してリリースし、フリーソフトウェアでのその利用を許可することを推奨します。